UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/067,403	02/07/2002	Laurence Hamid	IVPH-0072	7278

23377 7590 09/07/2006

WOODCOCK WASHBURN LLP
ONE LIBERTY PLACE, 46TH FLOOR
1650 MARKET STREET
PHILADELPHIA, PA 19103

EXAMINER	
ABRISHAMKAR, KAVEH	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 09/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/067,403	HAMID, LAURENCE	
	Examiner	Art Unit	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 June 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 3-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 and 3-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on June 26, 2006 has been entered.

Response to Arguments

2. Applicant's arguments filed June 26, 2006 have been fully considered but they are not persuasive for the following reasons:

Regarding claim 1, the Applicant argues that the Cited Prior Art (CPA), Lockhart et al. (U.S. Patent 6,230,272), does not teach "decoding of the same security data." The Applicant argues that the CPA does not teach that the same security data is encoded with several different data keys to provide several different encoded secure data, which is later decoded. These arguments are not found persuasive. The system, in the preferred embodiment, is used to protect private keys of users by using a multipurpose data string, which is used as a seed, to form a symmetric key which is used for encryption of the security data (column 5 lines 7-13). This security data could

bed a private key of a user, or it could be any security data (column 7 lines 33-35), which could be a same security data which is accessible by a group of users that have the correct personal identification numbers (column 7 lines 1-7). This is analogous to the user authorization process (entering the PIN) and the one data key (multipurpose string) being used to decode the security data.

The Applicant argues that the CPA, Bjorn (U.S. Patent 6,035,398) and Gressel (U.S. Patent 6,311,272), do not teach the limitation of using "several different data keys ... such that a combination of user authorization and any of said different data keys allow for retrieval and decoding of the same security data." This argument is moot as Lockhart is being used as the primary reference in combination with Bjorn and Gressel as given below.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1, 3-5, and 22-25 are rejected under 35 U.S.C. 102(e) as being anticipated by Lockhart US (6,230272).

Regarding claim 1: Lockhart discloses a method of securing security data stored on a computer system (see abstract) comprising the steps of:

Providing one of several different data keys to the computer system; (Col 3, lines 39-46);

Transforming the security data with the data key in a reversible fashion to produce encoded secure data such that the data key is required in order to perform a reverse transform and extract the security data from the encoded secure data; and (Col 4, lines 35-43)

storing the encoded secure data in a fashion such that a user authorization process is used to retrieve the encoded secure data such that the data key and the user authorization process in combination, provide access to the security data and such that the stored data within the computer system is encoded. (Col 4, lines 43-45 and Col 4, lines 59-65),

wherein a same security data is encoded with several different data keys to provide several different encoded secure data such that a combination of user authorization and any of a plurality of data keys allows for retrieval and decoding of the same security data (Col 5, lines 22-32 and Col 5, lines 52-62).

Regarding claim 3: Lockhart discloses the method of securing security data stored on a

computer system according to claim 1, wherein each encoded secure data is associated with one or more user authorization processes such that a combination of one or more user authorization processes and any of said several different data keys allows for retrieval and decoding. (Col 6, lines 8-24 and Col 7, lines 22-27)

Regarding claim 4: Lockhart discloses the method of securing security data stored on a computer system according to claim 1, wherein the user authorization process is a biometric information verification process. (Col 3, lines 45-49)

Regarding claim 5: Lockhart discloses the method of securing security data stored on a computer system according to claim 1, wherein the data keys include a password. (Col 4, lines 3-8).

Regarding claim 22, Lockhart discloses:

A computer system that secures security data stored therein, comprising:

an input device that provides at least one of several different data keys to the computer system (Col 3, lines 39-46);

a processing device that encodes a same security data with said several different data keys in a reversible fashion to produce several different encoded secure data and such that respective ones of the several different data keys are required to perform a reverse transform and extract the security data from the encoded secure data (Col 4, lines 35-43);

a memory device that stores the encoded stored data(Col 4, lines 35-43); and

a user authorization process that retrieves the encoded secure data from the memory device such that at least one of the several different data keys and the user authorization process, in combination, provide access to the security data, wherein a combination of user authorization and any of said several different data keys allows for retrieval and decoding of the same security data (Col 5, lines 22-32 and Col 5, lines 52-62).

Regarding claim 23, Lockhart discloses:

A computer system according to claim 22, further comprising a plurality of authorization processes, wherein each encoded secure data is associated with one or more user authorization processes such that a combination of one or more user authorization processes and any of said several different data keys allows for retrieval and decoding of the security data (Col 6, lines 8-24 and Col 7, lines 22-27).

Regarding claim 24, Lockhart discloses:

A computer system according to claim 22, wherein the user authorization process is a biometric information verification process (Col 3, lines 45-49).

Regarding claim 25, Lockhart discloses:

A computer system according to claim 22, wherein the data keys include a password (column 6 lines 28-41).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 6-10, 13-15, and 18-21, 26-30, 33-3, and 37-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lockhart et al. (U.S. Patent 6,230,272) in view of Bjorn (U.S. Patent 6,035,398).

Regarding claims 6,13,19, 26, 33, and 38 Lockhart discloses:

A method of securing security data stored on a computer system comprising:

providing a biometric information source (Col 5, lines 61-64) and comparing the biometric information source against stored templates associated with the biometric information source;(Col 5, lines 64-68) and for, in dependence upon a comparison result pairing biometric information source with a first individual identity;(Col 6, lines 1-3);

providing one of several different data keys associated with the first individual identity (Col 3, lines 39-46) the one data key being other than stored on the computer system (Col 3, lines 39-46));

retrieving encoded security data associated with the information, and using the one data key for decoding the encoded security data. (Col 4, lines 43-45 and Col 4, lines 59-65),

wherein a same security data is encoded with several different data keys to provide several different encoded secure data such that a combination of user authorization and any of a plurality of data keys allows for retrieval and decoding (Col 5, lines 22-32 and Col 5, lines 52-62).

Lockhart does not explicitly disclose providing a biometric information source and comparing the biometric information source against stored templates associated with the biometric information source and for, in dependence upon a comparison result pairing biometric information source with a first individual identity. Bjorn teaches providing a biometric information source (Col 5, lines 61-64) and comparing the biometric information source against stored templates associated with the biometric information source;(Col 5, lines 64-68) and for, in dependence upon a comparison result pairing biometric information source with a first individual identity;(Col 6, lines 1-3). Lockhart and Bjorn are analogous arts as both are directed towards generating keys that are used to secure information. Furthermore, Lockhart anticipated the use of biometrics such as a fingerprint reader to identify the user. It would have been obvious to use a biometric source and comparing the biometric identity because using a biometric to create a key because it provides "a secure cryptographic key that is easily usable by the user, but not accessible to third parties."

Regarding claims 7, 18, and 27 Lockhart discloses:

A method of securing security data stored on a computer system according to claim 6, wherein the decoded security data is for performing at least one of encrypting and decrypting data on the computer system (Col 6, lines 8-24 and Col 7, lines 22-27).

Regarding claims 8 and 28: A method of securing security data stored on a computer system according to claim 6, wherein the decoded security data is for allowing access of the data to the identified individual. (column 7 lines 1-20).

Regarding claims 9 and 29, Lockhart does not explicitly disclose that the step of accepting the biometric source is using a contact imager. Bjorn discloses a method of securing security data stored on a computer system according to claim 6, wherein the step of accepting biometric information source comprises imaging the biometric information source using a contact imager. (Col 3, lines 4-11 and Col 4, lines 4-11). Lockhart and Bjorn are analogous arts as both are directed towards generating keys that are used to secure information. Furthermore, Lockhart anticipated the use of biometrics such as a fingerprint reader to identify the user. It would have been obvious to use a biometric source and comparing the biometric identity because using a biometric to create a key because it provides "a secure cryptographic key that is easily usable by the user, but not accessible to third parties."

Regarding claims 10 and 30, Lockhart does not explicitly disclose that the contact imager is a fingerprint imager. However, Bjorn discloses a method of securing security data stored on a computer system according to claim 9, wherein the contact imager is a fingerprint imager (Col 3, lines 4-11 and Col 4, lines 4-11). Lockhart and Bjorn are analogous arts as both are directed towards generating keys that are used to secure information. Furthermore, Lockhart anticipated the use of biometrics such as a fingerprint reader to identify the user. It would have been obvious to use a biometric source and comparing the biometric identity because using a biometric to create a key because it provides "a secure cryptographic key that is easily usable by the user, but not accessible to third parties."

Regarding claims 14, 21, and 34, Lockhart does not disclose hashing the first information sample to produce a first hash value. However, Bjorn discloses the method of securing data as defined in claim 13, wherein the step of providing a first information sample to a computer system comprises: hashing the first information sample to produce a first hash value (Col 3, lines 44-59). Lockhart and Bjorn are analogous arts as both are directed towards generating keys that are used to secure information. Furthermore, Lockhart anticipated the use of biometrics such as a fingerprint reader to identify the user. It would have been obvious to use a biometric source and comparing the biometric identity because using a biometric to create a key because it provides "a

secure cryptographic key that is easily usable by the user, but not accessible to third parties."

Regarding claim 15, Lockhart does not disclose providing a second information sample, hashing the second information sample, and encoding the key data, and securing the second security data. Bjorn discloses the method of securing data comprising:

providing a second other information sample to the computer system;(Col 3, lines 28-36)

hashing the second information sample to produce a second hash value; (Col 3, lines 44-46)

encoding the key data in dependence upon the second hash value to produce second security data; and (Col 3, lines 54-65)

securing the second security data in dependence upon at least one of the at least one biometric information sample.(Col 4, lines 8-20).

Lockhart and Bjorn are analogous arts as both are directed towards generating keys that are used to secure information. Furthermore, Lockhart anticipated the use of biometrics such as a fingerprint reader to identify the user. It would have been obvious to use a biometric source and comparing the biometric identity because using a biometric to create a key because it provides "a secure cryptographic key that is easily usable by the user, but not accessible to third parties."

Regarding claims 20 and 39, Lockhart does not explicitly disclose the providing a first information sample and comparing the decoded biometric sample against stored templates. Bjorn discloses the method of securing data according to claim 19, comprises the steps of: providing a first information sample to a computer system for decoding the encoded biometric sample; (Col 4, lines 60-63 and item 340 of FIG. 3) and comparing the decoded biometric sample against stored templates associated with the

biometric information source. (Col 4, lines 64-67 and item 345 of FIG. 3). Lockhart and Bjorn are analogous arts as both are directed towards generating keys that are used to secure information. Furthermore, Lockhart anticipated the use of biometrics such as a fingerprint reader to identify the user. It would have been obvious to use a biometric source and comparing the biometric identity because using a biometric to create a key because it provides "a secure cryptographic key that is easily usable by the user, but not accessible to third parties."

Regarding claim 37, Lockhart discloses:

A computer system according to claim 33, wherein the encoding means encrypts data using the key data (column 6 lines 33-41).

3. Claims 11,12,16, 17, 31-32, and 35-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lockhart et al. (U.S. Patent 6,230,272) in view of Bjorn US (6,035,398) in further in view of Gressel US (6,311,272).

Regarding claims 11,16, 31, and 35 Lockhart and Bjorn disclose the method of securing security data stored on a computer system according to claim 6, wherein the step of providing the data key comprises the step of providing a public/private key pair (Col 8, lines 54-61) but he doesn't explicitly disclose the step of providing the data key comprises the step of providing. However, Gressel discloses a biometric authentication system where he teaches the using of a password or a shared secret to retrieve and

decrypt decryption key stored on memory using biometric techniques (Col 5, lines 56-65) . Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to modify Bjorn system with the teachings of Gressel to include provide a password through the authentication process. One would be motivated to do so in order to enable the system to provide the decryption key to the user by authenticating the user using a password or PIN that is usually easier for the user to remember and keeping the decryption key in a secure area.

Regarding claims 12, 17, 32, and 36, Lockhart and Bjorn disclose the method of securing security data stored on a computer system according to claim 6, wherein the step of providing the data key comprises the step of providing information stored on a database but he doesn't explicitly disclose the step of providing the data key comprises the step of providing information stored on smart card. However, Gressel discloses a biometric authentication system where he teaches storing decryption key on a smart card and using a shared key to retrieve and decrypt decryption key stored on the smart card (Col 3, Lines 50-55 and Col 8, lines 28-38). Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to modify Bjorn invention with the teachings of Gressel to provide a data key stored the smart card. One would be motivated to do so in order to eliminate any possibility of the decryption key being compromised during operation and to provide higher degree of security against physical attacks. Additionally using the smart card enables the system to provide a higher degree of mobility for the users.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KA
09/02/2006